WO

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Carol Davis, Plaintiff, vs. HDR Incorporated, Defendant.	No. CV-21-01903-PHX-SPL **ORDER**

Before the Court is Defendant HDR Incorporated's ("Defendant") Motion to Dismiss (Doc. 11), in which Defendant requests that this Court dismiss this action in its entirety. Defendant's Motion has been fully briefed and is ready for review. (Docs. 11, 13 & 14).[1] For the following reasons, Defendant's Motion will be granted.[2]

[1] The Court is also in receipt of Defendant's Request for Judicial Notice (Doc. 12), in which Defendant requests that the Court take judicial notice of four specific documents: (1) Facebook's Data Policy (Doc. 12 at 7–17); (2) Facebook's Group Privacy Settings (*Id.* at 19–21); (3) Facebook's Automatic Approval Setting (*Id.* at 23–24); and (4) an article from Vice.com (*Id.* at 26–31). Plaintiff does not dispute the documents Defendant references or otherwise object to Defendant's Request.

Therefore, the Court grants Defendant's Request and takes judicial notice of the documents referenced therein. *See* Fed. R. Evid. 201 (governing judicial notice); *Lee v. City of L.A.*, 250 F.3d 668, 688–90 (9th Cir. 2001) (discussing judicial notice in context of a motion to dismiss and noting that a court "may take judicial notice of 'matters of public record' without converting motion to dismiss into a motion for summary judgment").

[2] Because it would not assist in resolution of the instant issues, the Court finds the pending motion is suitable for decision without oral argument. *See* LRCiv. 7.2(f); Fed. R. Civ. P. 78(b); *Partridge v. Reich*, 141 F.3d 920, 926 (9th Cir. 1998).

I. BACKGROUND

Defendant HDR, Inc. is an architecture and design firm that has designed over 275 jails and prisons. (Doc. 1 at 5). In addition to its architectural services, Defendant offers its clients "strategic communications" services. (*Id.* at 5–6). These services involve gauging public sentiment and developing media campaigns to help clients manage the risks associated with proposed or existing projects. (*Id.*). Plaintiff Carol Davis' ("Plaintiff") allegations specifically relate to Defendant's "STRATA" service—a surveillance or "social listening" service that gathers social media data with the goal of "gaug[ing] and mitigat[ing] social and political risks before they affect a project." (*Id.*). Essentially, Defendant's STRATA service uses social media data to survey, evaluate, and determine trends in public opinion and to identify key influencers and the leadership of potential opposition groups and citizen activists. (*Id.* at 6–7). This information allows Defendant to track a project's success, identify potential risks, and measure the effectiveness of messaging and communication. (*Id.*).

This case involves two Facebook groups: "Ahwatukee411" and "Protecting Arizona's Resources & Children" ("PARC") (collectively, the "Groups"). (*Id.* at 8–9). Ahwatukee411 is a Facebook group "that enables local residents of the Ahwatukee Foothills area to privately discuss issues concerning the community." (*Id.* at 7–8). The group was formed around December 2014 and has approximately 32,400 members. (*Id.*). PARC is a Facebook group that was "formed to protest the construction of a highway that cuts through the Moahdak Do'ag Mountain (South Mountain) . . . [and] enables its members to privately discuss local issues." (*Id.* at 8). The group was formed around 2016 and has approximately 930 members. (*Id.*). Both Ahwatukee411 and PARC have "always been" private, closed Facebook groups—meaning only group members can access and see posts made within the Groups. (*Id.*). Both Groups require prospective members to undergo a screening process. (*Id.*). Ahwatukee411's screening process is "intended to ensure that only residents (*i.e.*, those with a vested interest in the Ahwatukee community) can join the group." (*Id.*). The intent of PARC's screening process is very similar: "to ensure that

largely only residents (*i.e.*, those whose homes would be affected by the construction of the local highway) can join the group." (*Id.*).

Plaintiff has been a member of Ahwatukee411 since approximately 2015 and a member of PARC since approximately 2016. (*Id.* at 9–10). Plaintiff alleges that she privately communicated with other members in the Groups and that such communications concerned topics such as "recommendations for services and debates over local issues, including the construction of a local highway [and its environmental impact,] and potential political corruption." (*Id.* at 10). Plaintiff alleges that she believed she was only communicating with other Ahwatukee residents or individuals whose interests aligned with the PARC organization's goals. (*Id.*).

Since at least 2016, Plaintiff alleges that Defendant infiltrated the Groups and generated "an 'influencer' report, an analysis of public sentiment on social media platforms, and a geospatial analysis that placed communities into categories." (*Id.* at 9). Plaintiff alleges that Defendant "tracked, read, intercepted, analyzed, and otherwise wiretapped and/or accessed in electronic storage" Plaintiff's private posts within the Groups, without her consent. (*Id.* at 10). On November 10, 2021, Plaintiff filed a Complaint against Defendant on behalf of herself and two purported classes of members of the Groups. (*Id.* at 10–11). The Complaint alleges four counts:

> (i) Interception and disclosure of electronic communications in violation of the Federal Wiretap Act, 18 U.S.C. § 2511;
>
> (ii) Manufacture, distribution, possession, and advertising of an electronic communication interception device in violation of the Federal Wiretap Act, 18 U.S.C. § 2512;
>
> (iii) A violation of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*; and
>
> (iv) Common law invasion of privacy/intrusion.

(*Id.* at 12–16). Defendant now moves to dismiss Plaintiff's entire complaint for failure to state a claim, pursuant to Federal Rule of Civil Procedure 12(b)(6). (Doc. 11).

///

II. LEGAL STANDARD

To survive a Rule 12(b)(6) motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A court may dismiss a complaint for failure to state a claim under Rule 12(b)(6) for two reasons: (1) lack of a cognizable legal theory, or (2) insufficient facts alleged under a cognizable legal theory. *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990). A claim is facially plausible when it contains "factual content that allows the court to draw the reasonable inference" that the moving party is liable. *Ashcroft*, 556 U.S. at 678. Factual allegations in the complaint should be assumed true, and a court should then "determine whether they plausibly give rise to an entitlement to relief." *Id.* at 679. Facts should be viewed "in the light most favorable to the non-moving party." *Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1019 (9th Cir. 2013).

III. DISCUSSION

Defendant moves for the dismissal of Plaintiff's claims. (Doc. 11 at 7, 21). Defendant first argues that Plaintiff's communications in the Groups were not private to begin with and are therefore not protected under the law. (*Id.* at 12–15). Second, Defendant argues that Plaintiff fails to plausibly allege essential elements with respect to each of her four claims. (*Id.* at 15–21). The Court will first address Plaintiff's claims under the Wiretap Act and the Stored Communications Act. Then, the Court will turn to Plaintiff's common law invasion of privacy claim.

A. Wiretap Act and Stored Communications Act Claims (Counts I–III)

With respect to Plaintiff's Wiretap Act and Stored Communications Act claims, Defendant's primary argument is that Plaintiff's posts in the Groups were not private communications because they were readily accessible to the general public—and that therefore her posts are not protected under the Acts. Defendant additionally argues that Plaintiff failed to plausibly allege the essential elements of her ECPA claims. The Court finds that Plaintiff's posts were not private, protected communications and therefore does

not reach Defendant's arguments concerning to the remaining elements of each claim.

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA") in an effort "to afford privacy protection to electronic communications." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). The ECPA encompasses both the Wiretap Act, 18 U.S.C. §§ 2510–2523, and the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–2713. The former protects communications *in transit* while the latter protects *stored* communications.[3] *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1042 (N.D. Cal. 2014). Specifically, the Wiretap Act "provides a private right of action against any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." *Id.* (internal quotations omitted) (citing § 2511(1)(a); § 2520 (creating private right of action)). The SCA, in contrast, provides a private right of action "where a person (1) intentionally accesses (2) a facility through which an electronic communication service is provided (3) without authorization or by exceed[ing] an authorization given and (4) thereby obtains . . . a wire or electronic communication (5) while that wire or electronic communication is in electronic storage." *Id.* at 1041 (internal quotations omitted) (citing § 2701(a); § 2707 (creating private right of action)).

Electronic communications which are "readily accessible to the general public" are explicitly exempted from protection under the Wiretap Act and the SCA. § 2511(2)(g). Specifically, the ECPA provides that

> [i]t shall *not* be unlawful under [the Wiretap Act] or [the SCA] for any person—(i) to intercept or access an electronic communication made through an electronic communication

---

[3] "[T]he intersection of [the Wiretap Act and the SCA] 'is a complex, often convoluted, area of the law.'" *Konop*, 302 F.3d at 874 (quoting *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998)). "[T]he difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication. . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results." *Id.* (citations omitted).

> system that is configured so that such electronic communication is *readily accessible to the general public*.

§ 2511(2)(g) (emphasis added). Although the Ninth Circuit has not addressed the "readily accessible" exception in great depth, the Eleventh Circuit has, and in doing so, found that it is not only an exception to protection under the statute, but also a required showing that is "material and essential to recovery under the [ECPA]." *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006). The Eleventh Circuit based this finding on the statute's overall structure and its legislative history, which "clearly show that Congress did not intend to criminalize or create civil liability for acts of individuals who 'intercept' or 'access' communications that are otherwise readily accessible by the general public." *Id.* at 1320–21. According to the Eleventh Circuit, requiring plaintiffs to show that their communications are not readily accessible by the general public is even *more* important in the context of electronic communications on the internet:

> Through the World Wide Web, individuals can easily and readily access websites hosted throughout the world. Given the Web's ubiquitous and public nature, it becomes increasingly important in cases concerning electronic communications available through the Web for a plaintiff to demonstrate that those communications are not readily accessible. If by simply clicking a hypertext link, after ignoring an express warning, on an otherwise publicly accessible webpage, one is liable under the [ECPA], then *the floodgates of litigation would open and the merely curious would be prosecuted*. We find no intent by Congress to so permit. Thus, the requirement that the electronic communication not be readily accessible by the general public *is material and essential to recovery* under the [ECPA].

Id. at 1321 (emphasis added). In *Snow*, the plaintiff failed to allege facts in his complaint from which a court could infer that his website was not readily accessible to the general public. *Id.* at 1321–22. As a result, the Eleventh Circuit upheld the lower court's grant of the defendants' motion to dismiss for failure to state a claim. *Id.* at 1322.

Here, Plaintiff argues that whether posts in the Groups were readily accessible to the public—and whether they are therefore private communications protected under the ECPA—is a factual dispute that must be construed in Plaintiff's favor at this motion-to-

dismiss stage. (Doc. 13 at 8). The Court does not agree. *Snow* clearly holds that the readily accessible issue concerns a "material and essential" element of an ECPA claim that must be sufficiently pleaded to in the complaint. *Snow*, 450 F.3d at 1321. This Court agrees with the Eleventh Circuit's reasoning and sees no reason to find differently. Moreover, this Court is unaware of—and Plaintiff has not shown—any authority suggesting that the readily accessible requirement is a factual issue. Therefore, to survive Defendant's Motion to Dismiss, Plaintiff's Complaint must allege facts, accepted as true, that are sufficient to conclude that her posts in the Groups were not readily accessible by the general public.

Courts have held that communications made on private websites, private electronic bulletin boards, and even one's own private Facebook wall may sometimes find protection under the ECPA. *See, e.g.*, *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668–69 (D.N.J. 2013) (holding posts on one's own, non-public Facebook wall are protected under the ECPA in part by analogizing to electronic bulletin boards). It appears that no court, however, has directly addressed the question presently before this Court: whether communications made in a "private" Facebook group[4] fall within the ECPA's protection. On one hand, it could be argued that posts in a private group are similar to posts on one's own Facebook wall. In both circumstances, only certain individuals—rather than the general public—are able to access and view the posts. Viewed this way, posts in a private group are not "readily accessible" to the general public and should be afforded ECPA protection. On the other hand, posts in a private group are unique in that the individual who creates the posts typically has no authority over who may become a member in the private group. The individual relinquishes control over who can access and view the post—in essence, the communication becomes "readily accessible" to the general public when it is posted in the group and cannot be protected under the ECPA.

Defendant, of course, argues the latter—that Plaintiff's posts in the Groups *were*

[4] When a Facebook group is designated as "private," only members of the group are permitted to see who is in the group, to post within the group, and to otherwise access and view communications in the group. (Doc. 12 at 19).

readily accessible to the public, regardless of the Groups' "nominal designation[s]" as "private" Facebook groups. (Doc. 11 at 13–14). According to Defendant, this is because joining the Groups was not overly restricted, the Groups' administrators—*and not Plaintiff*—had "unfettered discretion" over the Groups' access and privacy settings, and Plaintiff had no control over the dissemination of her posts outside the Groups. (*Id.*). Plaintiff responds by arguing that, by choosing to post in the Groups—which were designated as "private" and where access was limited by a screening process and posts were viewable only by Group members—Plaintiff "configured [her posts] in some way as to limit ready access by the general public." (Doc. 13 at 11). According to Plaintiff, this is all that the law requires for her posts to be considered private, ECPA-protected communications. (*Id.*).

The Eleventh Circuit's decision in *Snow* provides the Court a helpful starting point. In *Snow*, the plaintiff created his own non-commercial website intended as a "private support group" for individuals who had been sued by corporate entities. *Snow*, 450 F.3d at 1316. The website offered an electronic bulletin board which allowed its users to share messages with one another. *Id.* Access to the website was restricted and language on its homepage expressly prohibited access by Defendant DirecTV and its agents. *Id.* Users had to "register, create a password, and agree to additional terms that affirm[ed] the non-association with DirecTV." *Id.* Once a user completed those steps, he or she was allowed to enter the website and participate in its electronic bulletin board. *Id.* The plaintiff alleged that DirecTV employees accessed the website and viewed its electronic bulletin board on multiple occasions. *Id.* The plaintiff filed suit, asserting that the defendants' unauthorized access violated the SCA. *Id.*

As explained above, the Eleventh Circuit found that—in order to state a proper SCA claim and survive the defendants' motion to dismiss—the plaintiff must have alleged facts sufficient to infer that his electronic bulletin board was not readily accessible to the general public. *Id.* at 1321. The plaintiff failed to do so, because none of the access steps—registering, creating a password, and agreeing to terms of non-association with DirecTV—

permitted an inference that the general public was restricted. *Id.* at 1321–22. The Eleventh Circuit distinguished the case from *Konop*, 302 F.3d at 868, a Ninth Circuit decision that also dealt with a restricted, non-commercial website. *Id.* at 1322. In *Konop*, the plaintiff created a discrete list of individuals who were eligible to access his website. *Konop*, 302 F.3d at 872. To access the *Konop* website, one had to enter the name of an eligible individual, create a password, and click "SUBMIT" indicating their acceptance of certain terms and conditions which "prohibited any member of [the defendant]'s management from viewing the website and prohibited users from disclosing the website's contents to anyone else." *Id.* at 872–73. According to the Eleventh Circuit, the key distinction between the websites was that the *Konop* website—unlike the *Snow* website—"required users wishing to view the [website] to have knowledge (an eligible employee's name) *that was not publicly available*." *Snow*, 450 F.3d at 1322 (emphasis added). In contrast, the *Snow* website could essentially be viewed by anyone—a user did not have to have non-public knowledge of a particular individual's name. *Id.* The Eleventh Circuit characterized the *Snow* website's comparably minimal access restrictions as "a self-screening methodology by which those who are not the website's intended users would voluntarily excuse themselves." *Id.* The Eleventh Circuit cautioned that the "readily accessible" requirement is not overly burdensome, and a plaintiff is not required "to 'plead in grave detail' all of a website's restrictive technical configurations." *Id.* Rather, a plaintiff need only show that the website is "configured in some way so as to limit ready access by the general public." *Id.* As an example, the Eleventh Circuit noted that "a short simple statement that the plaintiff screens the registrants before granting access may have been sufficient." *Id.*

In the present case, this Court finds that the access restrictions associated with the Groups are more akin to the restrictions imposed by the *Snow* website—even if they are not perfectly analogous. The Groups require prospective members to undergo a screening process that gauges their involvement and interest in the Ahwatukee community and the issues facing it. (Doc. 1 at 8). The Groups' administrators then presumably decide whether one's involvement and interest are sufficient for membership. (*See* Doc. 13 at 12 ("[T]he

administrators evaluate the results of the screening process to determine who is admitted to the private groups.")). In comparison, the *Snow* website required prospective users to affirm their non-association with DirecTV. *Snow*, 450 F.3d at 1316. The Eleventh Circuit found the *Snow* website's requirement to be "in essence, a self-screening methodology by which those who are not the website's intended users would voluntarily excuse themselves." *Id.* at 1322. Here, the requirement that prospective members disclose their involvement and interest in the community operates in a similar, "self-screening" manner: those who lack involvement or interest in the Ahwatukee community are unlikely to join the Groups and thus voluntarily excuse themselves. Moreover, the involvement and interest requirement—like the *Snow* website's requirement that one affirms their non-association with DirecTV—is distinguishable from the access requirement in *Konop* because it does not require a prospective member to have knowledge that is not available to the public.[5] In *Konop*, prospective users could access the website *only if* they entered the name of an individual whom the plaintiff website-creator had included on his eligibility list—a list that was not publicly available. *Konop*, 302 F.3d at 872. One who sought access to the *Konop* website *had* to know the name of an eligible individual; if he lacked such knowledge, access was prohibited. In contrast, one who seeks access to the Groups need only express some unspecified level of involvement or interest in the Ahwatukee community; if they do, they may become a member of the Groups. In other words, *any* person can become a member of the Groups, provided that they assert some unspecified level of involvement and interest in the community.

Plaintiff argues that the involvement and interest requirement asks *more* of

---

[5] The fact that prospective users do not have to disclose knowledge or private information not available to the public is *not* dispositive. As Plaintiff points out, the *Ehling* and *Crispin* cases serve as examples; in both cases, the users did *not* have to possess certain non-public knowledge to become Facebook friends with the plaintiffs and thereby access and view their private posts. Nonetheless, the courts in both cases held that the posts were protected by the ECPA. (Doc. 13 at 11). That said, the Court notes that the issue—whether one must have certain non-public knowledge to obtain access—was an important consideration in *Snow*, and it remains relevant and worthy of consideration in this case.

prospective members than does the "non-association with DirecTV" requirement in *Snow*. Whereas users of the *Snow* website merely had to "click a box" affirming their non-association with DirecTV, (Doc. 13 at 12), the Groups here have a specific screening process intended "to ensure that only residents (*i.e.*, those with a vested interest in the Ahwatukee community) can join the [Groups]." (Doc. 1 at 8). Plaintiff argues that the facts in this case "are exactly those which the court in *Snow* held would be sufficient for protection under the SCA (and the Wiretap Act)." (Doc. 13 at 12). Here, Plaintiff is alluding to the following excerpt from *Snow*:

> [A] short simple statement that the plaintiff screens the registrants before granting access may have been sufficient to infer that the website was not configured to be readily accessible to the general public.

(Doc. 13 at 12 (citing *Snow*, 450 F.3d at 1322)). Indeed, such a minimal screening process was missing from the *Snow* website, which permitted access to *anyone* so long as they registered and affirmed their non-association with DirecTV.

Here, it is true that access to the Groups involves a "screening process" that is more demanding than the mere checking of a box. That said, this Court finds that the screening process here is not the sort of screening process that *Snow* had in mind. *Snow* envisioned a screening process overseen by *the plaintiff*, *i.e.*, the individual asserting that his or her privacy rights were violated. *See id.* (emphasis added) ("[A] short simple statement that *the plaintiff* screens the registrants before granting access may have been sufficient."). Indeed, "[t]he language of the [ECPA] makes clear that the statute's purpose is to protect information that *the communicator* took steps to keep private." *Ehling*, 961 F. Supp. 2d at 668 (emphasis added); *see also Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 990 (C.D. Cal. 2010) (emphasis added) (analogizing Facebook wall postings to private YouTube videos because "both are accessible to a limited set of users *selected by the poster*"). This reading of the *Snow* excerpt is consistent with *Konop*, where it was *the plaintiff website-creator* who created the list of individuals who were eligible to access the website and who was therefore in sole control of access. *Konop*, 302 F.3d at 872. Here, it

is not Plaintiff who screens prospective members and determines whether they may be granted membership. Instead, it is the Groups' administrators who conduct such screening and who act as the ultimate arbiter of membership. (*See* Doc. 13 at 12 ("[T]he administrators evaluate the results of the screening process to determine who is admitted to the private groups.")). In sum, the Court rejects Plaintiff's argument that the facts in this case present the situation contemplated in *Snow*.

Plaintiff's lack of control over access to the Groups is also what distinguishes this case from *Ehling* and *Crispin*, the two cases most heavily relied upon by Plaintiff. In *Ehling* and *Crispin*, the courts recognized that non-public Facebook wall posts are covered by the ECPA. *Ehling*, 961 F. Supp. 2d at 669; *Crispin*, 717 F. Supp. 2d at 980–82. Critically, however, both cases dealt with posts on one's *own* private Facebook wall, not posts made on the wall of a private Facebook *group*. In *Ehling*, the District of New Jersey first noted that "[c]ases interpreting the SCA confirm that information is protectable as long as *the communicator* actively restricts the public from accessing the information." *Ehling*, 961 F. Supp. 2d at 668 (emphasis added) (citations omitted). Applying this principle, the *Ehling* court found that posts on one's own Facebook wall are protected:

> Facebook allows users to select privacy settings for their Facebook walls. Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user. The Court finds that, when users make their Facebook wall posts inaccessible to the general public, the wall posts are "configured to be private" for purposes of the SCA. The Court notes that when it comes to privacy protection, the critical inquiry is whether Facebook users took steps to limit access to the information on their Facebook walls.

Id. The *Ehling* court also relied on *Crispin*'s reasoning, which analogized Facebook wall posts to posts on electronic bulletin board systems ("BBS"):

> To determine whether the SCA applied to these communications, [*Crispin*] analogized a Facebook wall post to technology that existed in 1986: a posting on a BBS. . . . A BBS could be configured to be public or private. . . . If a BBS was configured to be private, access to the BBS was restricted to a particular community of users, and the messages posted to the BBS were only viewable by those users. . . . The *Crispin* court

> recognized that there was a long line of cases finding that the SCA was intended to reach private BBS's. . . . The court then found that there was "no basis for distinguishing between a restricted-access BBS and a user's Facebook wall or MySpace comments": both technologies allowed users to post content to a restricted group of people, but not the public at large. . . . The court therefore concluded that, if the plaintiff's Facebook page was configured to be private, then his wall posts were covered by the SCA. . . . This Court agrees in all respects with the reasoning of *Crispin*.

Id. at 668–69 (internal citations omitted). *Ehling* ultimately held that the plaintiff's non-public Facebook wall posts were covered by the SCA "[b]ecause [she] chose privacy settings that limited access to her Facebook wall to only her Facebook friends."[6] *Id.* at 669.

In the present case, the Facebook posts at issue were not on Plaintiff's own private Facebook wall such that she retained control over who could access and view them. Instead, Plaintiff's posts were made in the Ahwatukee411 and PARC Facebook groups, forums over which Plaintiff had *no control at all*. Plaintiff had no authority over the Groups' privacy settings and no voice in the screening process used to determine membership. Plaintiff therefore had no control over who was granted membership to the Groups and no ability to limit access to her posts to particular groups or individuals. By choosing to post in the Groups, Plaintiff was not "actively restrict[ing] the public from accessing the information," *Ehling*, 961 F. Supp. 2d at 668. Rather, she was doing just the opposite—posting in a place where she had no ability to restrict access. This is distinctly different than the facts presented in any of the cases cited to by the parties. *See Ehling*, 961

---

[6] In responding to Defendant's argument that the number of members in the Groups is a relevant consideration, Plaintiff quotes *Ehling* as holding that "[p]rivacy protection provided by the SCA does not depend on the number of *members in the private Facebook groups*. *See Ehling*, 961 F. Supp. 2d at 668." (Doc. 13 at 14 (emphasis added)). Plaintiff, however, misquoted this phrase from the decision. *Ehling* instead holds that "[p]rivacy protection provided by the SCA does not depend on *the number of Facebook friends that a user has*." *Ehling*, 961 F. Supp. 2d at 668.

First, the Court does not appreciate Plaintiff's blatant misrepresentation of the caselaw. Second, Plaintiff's modification of the phrase to better match the facts in this case only serves to emphasize the important distinction between *Ehling* and the present case: whereas *Ehling* dealt with one's own private Facebook wall, the present case concerns a private Facebook group.

F. Supp. 2d at 668–69 (plaintiff retained absolute control over privacy status of posts because they were posted on her own, non-public Facebook wall); *Crispin*, 717 F. Supp. 2d at 980–82 (same); *Snow*, 450 F.3d at 1321–22 (plaintiff created website and had control over how it was accessed); *Konop*, 302 F.3d at 872–73 (same). Plaintiff fails to cite to—and this Court is itself unaware of—any decision where a court has held that the ECPA protects the communications of an individual who posted those communications in a forum over which the individual entirely lacks control over access.

Of course, it could be argued that an individual posting on the wall of a private Facebook group is at least taking *some* steps to limit general-public access to the post—after all, the individual is choosing to disseminate the communication to a discrete group of Facebook users rather than the public at-large. In this sense, the communication is similar to posting on one's own private wall because—at least at the moment of posting—the communicator is intending to proffer the post only to a select group of people. This view of the issue—focusing on the communicator's intent at the moment of posting—wholly sidesteps the issue of control over access to the Groups. Simply ignoring that issue, however, does nothing to solve the problems it raises. Without any control over access to the Groups, Plaintiff necessarily relinquished any ability to "actively restrict the public from accessing" the post. *Ehling*, 961 F. Supp. 2d at 668. There is nothing to impede the Groups' administrators—who *do* have such control (*see* Doc. 12 at 19, 23)—from modifying or eliminating altogether the Groups' access restrictions and allowing the general public to access and view the post.[7] In that scenario, Plaintiff's posts could be

[7] Plaintiff argues that the conduct of the Groups' administrators—specifically, that they have maintained the private status of the Groups since their inception—supports Plaintiff's claims and undercuts any assertion that the administrators have "unfettered discretion" over access to the Groups or that they may someday choose not to enforce the access requirements by "automatically granting requests to join the group." (Doc. 13 at 12). The Court is unpersuaded. Just because the Groups' administrators have not yet made the Groups "public" or otherwise opened access to them does not mean that the administrators cannot or will not do so tomorrow. In any event, what is important for purposes of this analysis is not how the administrators have restricted access to the Groups to this point, but rather that Plaintiff has no say in the matter in the first place.

accessed and viewed by individuals who were not members at the time Plaintiff made the posts. If Plaintiff's original intent—that the posts would be accessible only by those who were members at the time of posting—was all that mattered, then the posts would still be considered not "readily accessible" to the general public. The "new" members of the Groups could be liable under the ECPA, despite their otherwise proper admission as members. This strange result is avoided entirely if the "readily accessible" inquiry considers more than just the Plaintiff's original intent. The posts here would be considered "readily accessible" to the general public—and excluded from ECPA protection—because Plaintiff relinquished control over access to them when she posted in the Groups.

Plaintiff also raises arguments related to the ECPA's authorization and consent exceptions. *See* 18 U.S.C. § 2511(2)(d) (providing that it shall not be unlawful under Wiretap Act for a person "to intercept a . . . communication . . . where one of the parties to the communication has given prior consent to such interception"); § 2701(c)(1)–(2) (providing that SCA does not apply "to conduct authorized . . . by the person or entity providing a wire or electronic communications service . . . [or] by a user of that service with respect to a communication of or intended for that user").[8] Here, Plaintiff argues that Defendant "was not authorized to access the posts" in the Groups and that it "was never given consent to access the posts" either. (Doc. 13 at 10). Thus, Plaintiff argues that "the only logical conclusion is that Defendant gained access to [the Groups] through deceit and deception." (*Id.*). Plaintiff then cites to several cases standing for the proposition that, where a defendant asserts an authorization or consent defense in response to alleged ECPA violations, such defenses are undermined if the defendant engaged in deceptive conduct.

---

[8] While there may be some differences between the Wiretap Act's consent exception and the SCA's authorization exception, the Court finds that any such differences do not impact the present motion. *See Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014) ("There may be subtle differences between the consent exception to Wiretap Act liability and the authorization exception to SCA liability. However, the parties conceded, and the Court finds that for the purposes of the instant Motion, the question under both is essentially the same.").

(*Id.* at 10–11 (listing cases)). Although this contention from Plaintiff is well received, the Court is unsure how it changes the "readily accessible" analysis.

Even *assuming* that Defendant gained access to the Groups by "deceit and deception," as Plaintiff alleges, the issue remains that Plaintiff's posts were "readily accessible" to the public and therefore not protected under the ECPA. Defendant may very well have gained access to the Groups by misrepresenting its interest and involvement in the Ahwatukee community—or even by outright asserting that it was a Ahwatukee resident—but this does not necessarily mean that Defendant violated the ECPA if posts in the Group were not private, protected communications in the first place. In other words, both can be true: Defendant gained access to the Groups by deceit and deception, but Plaintiff's posts in the Groups were not private, protected communications. Plaintiff may also be correct that Defendant's "deceit and deception" undermines any authorization or consent defense that Defendant may have. As such, any affirmative defense arguments related to consent or authorization could be undermined by Plaintiff at trial, or presumably even precluded from trial altogether. However, Defendant's argument on this Motion—that the posts in the Groups were not protected, private communications in the first place—is entirely separate from any consideration of an authorization or consent defense. *See In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1041 (N.D. Cal. 2014) (rejecting plaintiffs' argument that their allegation of lack of consent suffices to state privacy claim because "the case law suggests that in determining whether a plaintiff has satisfied the elements of the claim, a plaintiff's lack of consent does not matter so much as the nature of the information in which he or she alleges a privacy interest").

In sum, the Court finds that Plaintiff has failed to plausibly allege facts that would allow this Court to infer that Plaintiff's posts in the Groups were "configured in some way so as to limit ready access by the general public." *Snow*, 450 F.3d at 1322. Rather, Plaintiff's factual allegations imply that she did the just the opposite by choosing to post her communications in forums over which she had no control of access restrictions and privacy settings. Plaintiff's Wiretap Act (Counts I–II) and SCA (Count III) claims must be

dismissed because Plaintiff failed to plausibly allege that her posts were not readily accessible by the general public, which is a required showing for any ECPA claim.

B. Common Law Invasion of Privacy Claim (Count IV)

Arizona follows the Restatement (Second) of Torts for invasion of privacy claims. *Hart v. Seven Resorts, Inc.*, 190 Ariz. 272, 279 (Ct. App. 1997). Courts traditionally recognize "four separate torts under the right to privacy: (1) intrusion on the plaintiff's seclusion or private affairs; (2) public disclosure of embarrassing private facts; (3) publicity placing the plaintiff in a false light in the public eye; and (4) appropriation of the plaintiff's name or likeness for the defendant's advantage." *Skinner v. Tel-Drug, Inc.*, No. CV-16-00236-TUC-JGZ (BGM), 2017 WL 1076376, at *4 (D. Ariz. Jan. 27, 2017) (citing *Godbehere v. Phx. Newspapers, Inc.*, 162 Ariz. 335, 338 (1989)). Here, Plaintiff's Complaint alleges only the first of these torts: intrusion upon seclusion. (Doc. 1 at 15–16).

A claim for intrusion upon seclusion requires the Plaintiff to prove two elements: (i) an intentional intrusion, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns and (ii) that the intrusion would be highly offensive to a reasonable person. *Hart*, 190 Ariz. at 279 (citing Restatement (Second) of Torts § 652B). To satisfy the first element, "a plaintiff must show: (a) an actual, subjective expectation of seclusion or solitude in the place, conversation, or matter, and (b) that the expectation was objectively reasonable." *Dible v. City of Chandler*, No. CV 03-00249-PHX-JAT, 2005 WL 8162952, at *8 (D. Ariz. Jan. 10, 2005) (citing *Med. Lab'y Mgmt. Consultants v. Am. Broad. Cos., Inc.*, 306 F.3d 806, 812–13 (9th Cir. 2002) (applying Arizona law)). "The Comments to the Restatement further define the contours of the tort:

> The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his

> wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents.

Liberty Life Ins. Co. v. Myers, No. CV 10-2024-PHX-JAT, 2011 WL 3297506, at *4 (D. Ariz. Aug. 1, 2011) (quoting Restatement (Second) of Torts § 652(B) cmt. b (1977)). "The restatement makes clear, however, that the tort arises only when a defendant intrudes upon a place of privacy or seclusion *established and maintained by the plaintiff*." *Maguire v. Coltrell*, No. CV-14-01255-PHX-DGC, 2015 WL 6168417, at *6 (D. Ariz. Oct. 21, 2015) (emphasis added). "The defendant is subject to liability . . . only when he has intruded into a private place, or has otherwise invaded a private seclusion *that the plaintiff has thrown about his person or affairs*." *Id.* (internal quotations omitted) (emphasis added) (citing § 652(B) cmt. c). Here, the Court finds that Plaintiff fails to plausibly allege the first element of the claim because the facts in the Complaint do not permit an inference that Defendant intruded into a private place when it allegedly accessed and viewed the posts in the Groups.

It is true that the Groups were designated as "private" Facebook groups. As a result, posts in the Groups—such as Plaintiff's—were only accessible by the Groups' members. It is also true that to become a member, one had to undergo a screening process that inquired into his or her involvement and interest in the Ahwatukee community and that was intended to ensure that only (or "largely only", in the case of PARC (*see* Doc. 1 at 8)) Ahwatukee residents were allowed to become members. However, these facts alone—even when viewed in the light most favorable to Plaintiff—fail to establish that Plaintiff had a reasonable expectation of privacy because, as discussed extensively above, Plaintiff had no control whatsoever over the privacy settings and access restrictions of the Groups. Plaintiff therefore had no control over who could access and view the communications she posted in the Groups. Instead, the Groups were accessible to all those who underwent the screening process and who were granted membership by the Groups' administrators. Plaintiff's communications were posted not in "a place of privacy or seclusion established and maintained by the plaintiff," *see Maguire*, 2015 WL 6168417, at *6, but rather in a place that was accessible by the public. *See Interscope Recs. v. Duty*, No. 05CV3744-PHX-

FJM, 2006 WL 988086, at *3 (D. Ariz. Apr. 14, 2006) ("[I]t is undisputed that the share file is publicly available, and therefore [the plaintiff] cannot show that the [defendant] intruded upon her private affairs."). This Court finds that Plaintiff relinquished any expectation of privacy in her online communications when she posted them in the Groups. Thus, even *assuming* Defendant gained access to the Groups by misrepresenting its interest, involvement, and residency in the Ahwatukee community, Defendant did not intrude upon a place of privacy or seclusion when it accessed and viewed Plaintiff's posts.

While Plaintiff may take issue with the allegedly deceitful manner in which Defendant gained access to the Groups, she has not plausibly alleged an invasion of privacy because she failed to show that she had a reasonable expectation of privacy in communications posted in forums over which Plaintiff had no ability to control access. Thus, the Court need not reach the question of whether her Complaint satisfactorily alleges the second element of the invasion of privacy claim—that is, whether Defendant's alleged invasion would be "highly offensive to a reasonable person."

IV. CONCLUSION

Leave to amend a deficient complaint should be freely given "when justice so requires." Fed. R. Civ. P. 15(a)(2). When dismissing for failure to state a claim, "a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122, 1130 (9th Cir. 2000) (internal quotation marks omitted). Here, the Court will grant Plaintiff's request for leave to amend.

///

///

///

///

///

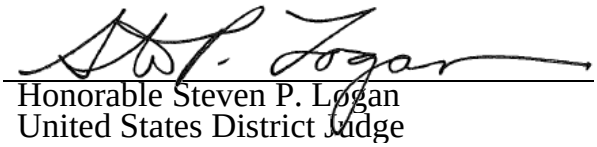
///

///

Accordingly,

IT IS ORDERED that Defendant HCR, Inc.'s Motion to Dismiss (Doc. 11) is **granted**. Plaintiff's claims are dismissed **without prejudice**. Plaintiff is granted leave to amend and may refile her Complaint if she believes that an Amended Complaint would sufficiently state the claims in accordance with this Order.

Dated this 8th day of June, 2022.



Honorable Steven P. Logan
United States District Judge